Willison R, Lowry P.

Disentangling the Motivations for Organizational Insider Computer Abuse through the Rational Choice and Life Course Perspectives.

***The Data Base for Advances in Information Systems* 2017, 49(1), 81-102.**

Disentangling the Motivations for Organizational Insider Computer Abuse through the Rational Choice and Life Course Perspectives

ABSTRACT

Criminal organizational insider computer abuse (ICA) research has focused on factors that influence either ICA intentions, or actual behavior during the ICA process. However, this research has failed to correctly conceptualize the decision-making processes involved in ICA. Thus, our first aim is to demonstrate this current deficiency by leveraging the rational choice perspective (RCP) from criminology. The RCP advances an "event" stage, in which choices are made leading up to and during the criminal act. However, the RCP also acknowledges a preceding "initial involvement" stage, which encompasses those factors that lead an individual to consider participation in crime. RCP explains that if, during the initial involvement stage, an individual becomes motivated and decides that future criminal behavior is the most suitable course of action, then he or she will have reached a state of "readiness." It is only after an individual has become readied, and at a later time, does the individual make event decisions in the perpetration of a specific crime. Consequently, extent ICA research has overlooked consideration of why—prior to the crime-an individual initially considers engaging in such criminal activity in the first instance. And, this is not to be conflated with intentions. Accordingly, we argue that there needs to be a clear distinction between those motivational factors that would lead to the consideration of such engagement at the initial involvement stage, and those factors that would lead an individual at the event stage to perpetrate a crime. We thus propose a revised version of the extended security action cycle (ESAC), which reflects these criminal decision-making stages. Moreover, we provide a means through which to identify and understand the relationship among those factors that may motivate an individual during the initial involvement stage, by drawing on the life course perspective (LCP). With a focus on time, context, and process, the LCP offers a framework in which are inscribed four key principles. Through examples drawn from the LCP and white-collar crime literature, we illustrate how these principles can provide a basis for conceptualizing factors that motivate ICA and open up new avenues for future research/theory development.

Disentangling insider computer abuse.

KEYWORDS

Computer abuse (CA), insider computer abuse (ICA), life course perspective (LCP), rational choice perspective (RCP), deterrence, employee computer abuse, organizational security, organizational insider, future directions for IS security research.

INTRODUCTION

Although hackers and viruses often dominate the media headlines regarding security breaches, information systems (IS) security practitioners also have to deal with a range of threats from inside their organizations. Long before the international incidents involving Private Manning (U.S. military intelligence leaks to Wikileaks) and Edward Snowden (The U.S. National Security Agency document leaks), experts concurred that organizational insiders represent the greatest threats to IS security, and this assessment applies equally today (Crossler et al., 2013; Vance et al., 2013). The threat exists because insiders require broad access to the most valuable organizational information to perform their jobs effectively, and they often cannot be controlled through technical means alone (Vance et al., 2013). Moreover, such people literally have "insider" information not available externally that can be tempting to use for personal gain through such avenues as insider trading, fraud, and selling trade secrets (Cummings et al., 2012).

Attempts to gather accurate statistics on this pervasive insider problem are hampered by the fact that organizations often fail to report such crimes because they fear reputational damage, drawing attention to potential weaknesses, losing competitive advantage, and exposing privacy issues. Nonetheless, industry surveys provide some insight into the prevalence of insider computer abuse (ICA). The 2014 PricewaterhouseCoopers (PwC) global report on organizational security (2014) documented an increase of 51% in security budgets and a 25% increase in security incidents from 2013. Moreover, approximately 31% of security incidents likely were committed by current employees, 27% by former employees, 16% by current consultants or service providers, and 13% by former consultants or service providers. The survey makes clear that the insider threat is worsening over time and remains to be addressed sufficiently. Summarizing global concerns on the threat from insiders, chief security officer Michael A. Mason noted, "I see the insider threat looming larger in my windshield than in the past. . .. Our problems are more human than technological" (PwC, 2014, p. 8). More recently, PwC, CSO Magazine, The CERT Division[i] of the Software Engineering Institute at Carnegie Mellon University, and The United States Secret Service all teamed up to study organizational security issues. Aside from finding that approximately 23% of cybercrimes are

committed by organizational insiders, that these acts are exceedingly expensive and damaging, that 76% of CEOs are more worried about cybersecurity than the year before, that security incidents in up 28% in 2014 from 2013, that spending on cybersecurity has greatly increased, they grimly conclude that progress on thwarting such abuses has largely stalled (Anonymous, 2015).

Despite the substantial threat that ICA poses to organizations and the dire extant situation that efforts to thwart it have floundered, the response from IS security researchers can be most positively described as "modest." The few studies include (Harrington, 1996; Hu et al., 2011; Lee et al., 2004a; Lowry et al., 2014; Peace et al., 2003; Posey et al., 2011; Willison et al., 2016; Workman, 2007); whereas, scores of studies have examined noncriminal security intentions and behaviors. Appendix A provides a complete review of the ICA literature. Indeed, given the paucity of such studies, recent work has urged that greater focus be placed on the insider threat (Crossler et al., 2013; Posey et al., 2013; Willison & Warkentin, 2013). Mahmood et al. (2010), for example, likened the relationship between those responsible for enhancing security and those attempting to bypass it to the white hat/black hat (good guy/bad guy) distinction in Wild West movies. They noted how the IS security discipline has been dominated by "good guy white hat" approaches, which address issues such as employee compliance to IS security policies. As an alternative, they called for IS security academics to consider the "harder to reach black hat" subjects research. Such studies, they argued, will allow the development of more effective countermeasures based on better understandings of offender behavior. Even still, when considering "black hats" most researchers deal with external actors, such as hackers, and largely overlook malicious insiders who can do just as much damage or more.

To aid our examination of the insider threat, we discuss, challenge, and improve upon the existing literature by developing the extended security action cycle (ESAC) framework by Willison and Warkentin (2013), which they adapted from Straub and Welke (1998) (see Figure 1). Willison and Warkentin (2013) argued for the need to examine not only intention to undertake ICA and deterrence of such behavior, but also phenomena that temporally precede these areas. Specifically, they advocated examination of the thought processes of a potential rogue member of staff as well as their interaction within the organizational context. Furthermore, they asserted that, in certain

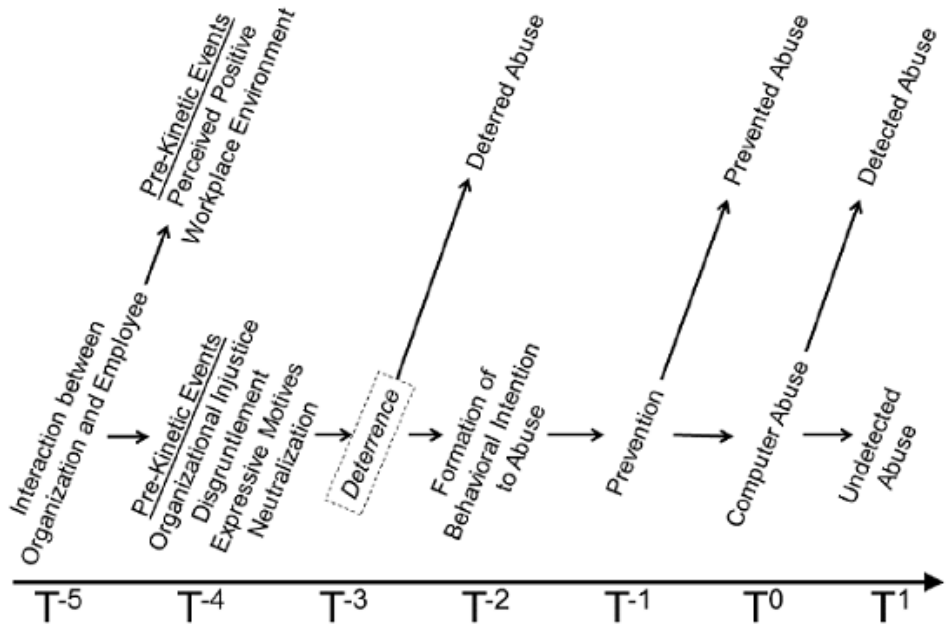

Figure 1. Extended Security Action Cycle, Electronically Reproduced from Straub and Welke (1998)

situations, such interactions might influence these thought processes and, consequently, influence the efficacy of deterrence safeguards.

Although we agree with the need to examine behavior which precedes the deterrence influence, we argue that the Willison and Warkentin (2013) article and related studies have insufficiently conceptualized the offender decision making processes for ICA. The existing studies have assumed that the only decision made is regarding the crime itself, often using the intention construct as a proxy for actual behavior. However, this understanding of ICA runs contrary to an established body of criminological research, which illustrates that an offender makes a series of choice in the criminal decision making process (Blumstein, 1986; Blumstein et al., 1988; Clarke & Cornish, 1985; Cornish & Clarke, 2013; Paternoster, 1989a, 1989b). Research by Blumstein (1986) and Blumstein et al. (1988), for example, highlighted the decisions made in a criminal career. In this context, the term "career" is not referring to the earnings involved to sustain a criminal's livelihood, but rather the sequence of decisions made in a period in which an offender is criminally active. Thus, there will be choices regarding the beginning (i.e., onset), the duration (i.e., career length) and cessation (i.e., the ending of criminal activities). Coupled with these decisions are choices made

regarding the frequency of offending, such as the number of times a criminal commits an offence.

In a similar vein, Clarke and Cornish (1985) and Cornish and Clarke (2013) advanced their "rational choice perspective" (RCP) on offender decision making. RCP clarifies that criminals make decisions regarding what are termed *involvement* and *event* stages. Similar to Blumstein (1986) and Blumstein et al. (1988), the involvement stages requires offender decisions to be made regarding initial involvement, continuation and desistance. Moreover, the "event" stage, involves offender choices leading up to and during the criminal act.

With specific relevance to the current discussion are the initial event and event stages advanced by Clarke and Cornish. Again, the "event" stage, involves offender choices leading up to and during the criminal act. Obvious parallels exist between the RCP and IS security research on ICA. However, the RCP also acknowledges the preceding "initial involvement" stage. RCP explains that if an individual becomes motivated during this stage and decides that future criminal behavior is the most suitable course of action, then he/she will have reached a state of "readiness." As Clarke and Cornish (1985, p. 167):

> *"Readiness involves rather more than receptiveness: it implies that the individual has actually contemplated this form of crime as a solution to his needs and decided that under the right circumstances he would commit the offence."*

Consequently, it is only later, during the criminal "event" stage, that a crime will be enacted. Given that the "initial involvement" stage has been over-looked in IS Security research, it has wrongly been assumed that any motivations are solely related to the criminal act. Yet, this assumption denies any consideration of why an individual would initially consider engaging in criminal activity in the first instance and the associated motivational influences. We, therefore, argue that there needs to be a clear distinction between motivational factors at the "initial involvement" stage and factors that would lead an individual to undertake a crime at the "event" stage.

As the distinction between initial involvement and event decisions has not been considered in current IS security research, this further calls into question the accuracy and utility of the ESAC. In their paper, Willison and Warkentin (2013) discussed "pre-kinetic" events, which temporally occur prior to deterrence influences. Thus, it is argued that three "event" types—namely, (1) organizational

justice disgruntlement, (2) expressive motives, and (3) neutralization—influence the efficacy of deterrence safeguards. However, the ESAC model only considers these types in terms of the criminal act (i.e., the event stage). We thus argue that the model conflates aspects of the criminal decision making process, by including factors, that from an RCP, would be categorized as relating to the "event," but also the "initial involvement" stage. For example, organizational justice disgruntlement from an RCP would be considered a motivational influence at the "initial involvement" stage. Our reasoning behind this argument is discussed in length in Section 3, in which we propose our revised version of the ESAC model, entitled The Two-Stage Decision-Making Process for ICA (Figure 4), based on the RCP.

Aside from acknowledging motivational factors at the initial involvement stage, there is also the obvious need to identify and understand them. Accordingly, we propose a framework based on the life course perspective (LCP). LCP affords a focus on time, context, process, and a framework for researching criminal phenomena. LCP encompasses a series of principles that guide LCP research, which we propose as the basis for studying motivational factors at the initial involvement stage.

In the remainder of this manuscript, we first provide further background information on ICA and the associated literature, and in doing so, we propose an improved definition of ICA. Next, we propose and advance our revised model of the ESAC, which is grounded in our observation that IS security studies on ICA have overlooked the initial involvement stage. We then address the problem of how to identify and understand those factors that may motivate an individual at the initial involvement stage. To assist in the identification and understanding of the relevant factors, we propose a new framework based on the LCP principles. We then describe each principle and illustrate how they may be applied to the information systems (IS) context. Finally, we conclude by considering the ICA research agenda and offer three potential avenues for future studies based on our conceptual work.

2. DEFINING ICA

In this section, we first explain ICA, using the associated literature. Generally, *computer abuse* (CA) is the deliberate and unauthorized misuse of information system assets (Posey et al.,

2011) whether by internal or external actors (Straub, 1990). However, our focus is on internal abuse that is intentional and criminal. Most studies in this domain have considered ICA, *internal computer abuse, computer abuse*, and *employee computer abuse* to be synonymous (e.g., D'Arcy et al., 2009b; Herath & Rao, 2009; Lowry et al., 2014; Posey et al., 2011); however, such terminological equivalence is not entirely accurate. We thus return to the literature to review the foundation of CA and ICA, propose an updated taxonomy for CA, and suggest a more precise definition of ICA.

To better define ICA we return to the work of Loch et al. (1992) who proposed the IS Security Threat Vector Taxonomy, which was revised slightly by Willison and Warkentin (2013). We have updated this taxonomy to better account for the security conditions in today's environment, and we use this taxonomy to define further what ICA is and is not.

Figure 2 depicts our updated IS Security Threat Vector Taxonomy. ICA involves employees or organizational insiders—not consumers or students. Thus, we assert that several studies about various unethical or risky computer behaviors involving consumers or students do not constitute ICA, including piracy of software and digital media (Lowry et al., 2017; Nandedkar & Midha, 2012); illegal peer-to-peer file sharing (Moore & McMullan, 2004); deviant computer behavior by students (Rogers et al., 2006); cyberslacking outside of work (Nandedkar & Midha, 2012); cyberbullying outside of work (Lowry et al., 2016); compulsive and deviant social networking behavior (James et al., 2017); organizational-level decisions to commit ethical breaches (Wall et al., 2016); and risky behaviors that create susceptibilities to malware, phishing, privacy violations, and identity theft (Keith et al., 2013; Lai et al., 2012; Salleh et al., 2012; Zhang et al., 2013).

We consider ICA to involve only malicious behaviors conducted by employees or other insiders in an organizational context. Furthermore, ICA does not involve an external threat. External threats to IS include human sources (e.g., hackers, crackers, social engineers, phishers, and cyberterrorists) (Bachmann, 2010; Bossler & Burrus, 2011; Hansen et al., 2007; Workman, 2008) and nonhuman sources (e.g., natural disasters, malware). It should be noted that the issue of organizational insiders in undermining security has grown more complex since Loch et al. (1992) published their article. Organizations today pursue workers in more virtual and temporary roles; thus, contractors,

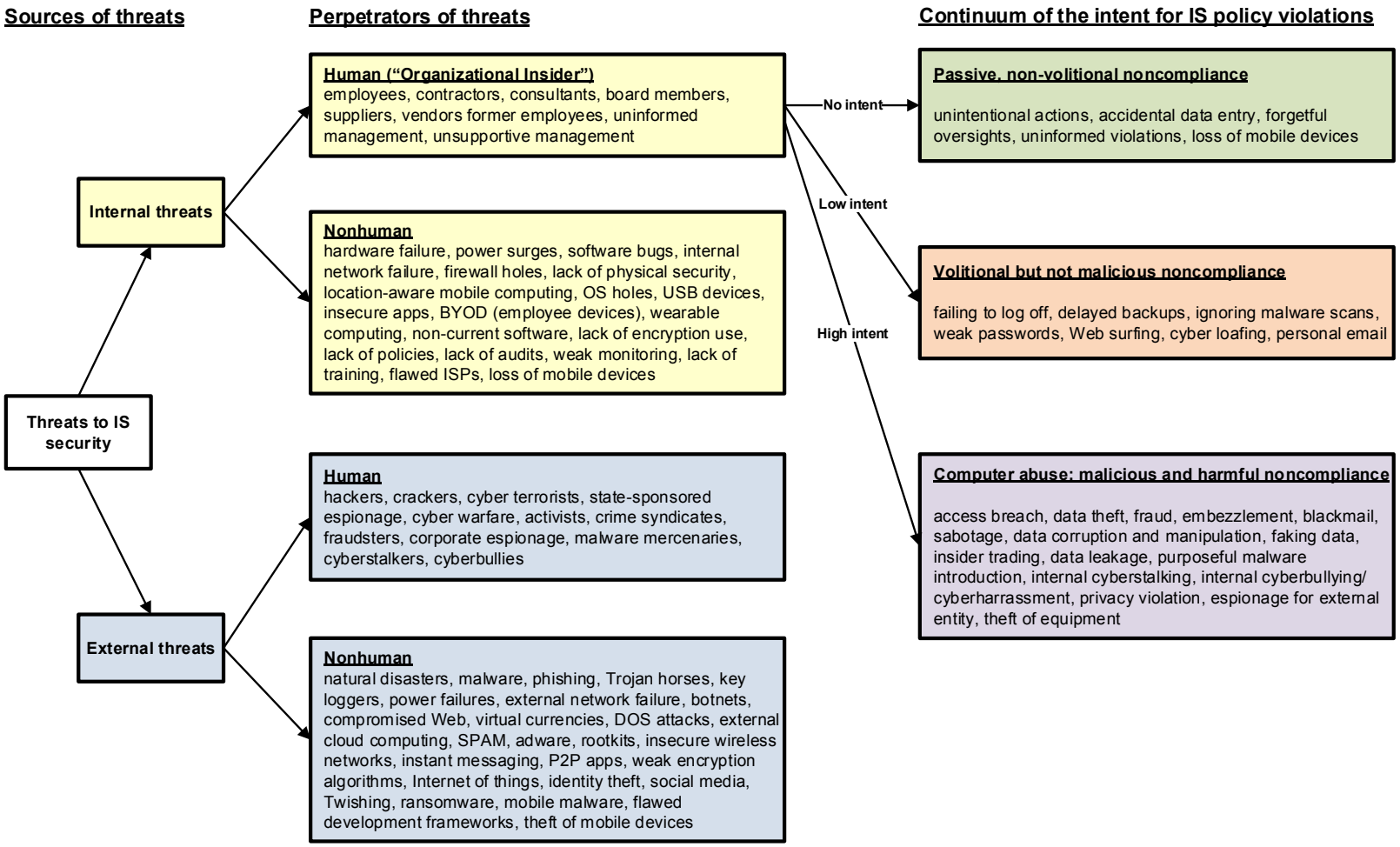

Figure 2. Our Updated IS Security Threat Vector Taxonomy, Adapted from Willison and Warkentin (2013)[ii]

consultants, and outside suppliers expand and complicate the category of organizational insiders. Moreover, the velocity of change in organizations has increased—today's employees are less likely to stay with the same organization for as long as employees of the past did—making former employees a greater threat.

We next leverage the taxonomy by Loch et al. (1992) for guidance as to when such internal threats are ICA. The key here is the *intent* of the IS policy violations. The taxonomy groups intent into threat categories: (1) passive, non-volitional noncompliance (e.g., accidental behaviors, uninformed violations, unintentional actions); (2) volitional but not malicious noncompliance (e.g., failing to backup data, not changing passwords regularly, not signing out of the system, security lapses) (Guo et al., 2011; Jenkins et al., 2014; Workman et al., 2008); and (3) internal, malicious and criminal computer abuse by employees or other insiders (e.g., sabotage, data theft, fraud, and deliberate policy violations but only those that are criminal) (e.g., Hu et al., 2011). We consider only this latter category ICA. For the second category, we also add newer behaviors, such as non-work related computing and cyberloafing that violates IS policies but are devoid of malicious deviant intent (e.g., surfing, personal email, shopping) (Lee et al., 2004b; Moody & Siponen, 2013).

We supplement the third category with newer phenomena that increasingly vex organizations. These criminal ICA behaviors include purposeful sharing or leaking of confidential organizational information or trade secrets (Smith et al., 2012); contravention of organizational security measures, including insider social engineering (Workman, 2007); and unauthorized data access or intentional access policy violations that are criminal (Hu et al., 2011). Moreover, employees are increasingly turning to social media at work, or using work resources, to commit newer criminal acts such as sexting, cyberbullying, cyberharassment, and the like—all of which has increased exposure and liability to organizations that need to be addressed and thwarted (Lowry et al., 2016). Aside from the obvious organizational issues that employee cyberbullying has caused, such as between employees, it turns out that organizations are also being held legally liable for the emotional and psychological damage that their employees inflict on those outside their organization, when such harassment is conducted using organizational resources, regardless of where it is done (Lowry et al., 2016).

Given our review of the CA and ICA literature, and the important distinctions between criminal and non-criminal security violations, we thus define *ICA* formally as follows:

> *"Intentional employee or other-insider behavior involving an organization's information assets or computing infrastructure that includes purposeful, deviant, and malicious intent against the best interests of an organization or its members, and which behavior is formally considered illegal."*

Given this enhanced definition of ICA, it should be clear that not all violations of an organization's IS security (IS policies) constitute ICA. For example, suppose an organization's IS policies state that employees must take care to run anti-malware on all email attachments. If an employee does not run anti-malware software on an email because he or she is in a hurry, this action is not considered ICA because there was no malicious intent and there is no criminal violation. However, if an employee was to forward a virus to a co-worker intentionally as an act of bullying or sabotage, such an act constitutes ICA.

3. THE COMPUTER ABUSE TIME LINE REVISITED

Given our review and improved definition of ICA, we now revisit and propose revisions to the computer abuse time line from the ESAC framework by Willison and Warkentin (2013), as they adapted it from Straub and Welke (1998) (see Figure 1). Willison and Warkentin considered three types of "pre-kinetic" events: (1) organizational justice disgruntlement, (2) expressive motives and (3) neutralization. They argued that these three types of events impact the efficacy of deterrence safeguards. However, the ESAC model only considers these three types in terms of the criminal act (i.e., during the "event" stage). Accordingly a fundamental flaw of the Willison and Warkentin model is that it conflates aspects of the criminal decision making process that from an RCP would be considered to be related to the event stage, but also the initial involvement stage. For example, organizational justice disgruntlement would be considered a motivational influence at the initial involvement stage, from an RCP. It is for this reasons that we propose key time line changes for implementation, including $T\text{-}^{3}$ and what precedes this point in time.

As noted, we based the aforementioned changes to the ESAC time line on the criminological research of Clarke and Cornish, who emphasized that (1985, p. 164):

> *"There is a fundamental distinction to be made between explaining the involvement of particular individuals in crime and explaining the occurrence of criminal events."*

Thus, Clarke and Cornish distinguished between *involvement* and *event* decisions. *Involvement decisions* relate to the three stages of a criminal career: An individual must make decisions about embarking on criminal activities (i.e., *initial involvement*), whether to continue these activities over time (i.e., *continuation*), and when, if at all, to cease offending (i.e., *desistance*). Event decisions refer to those decisions made during the commission of a crime.

Importantly, Clarke and Cornish (1985) depicted these decision stages in a series of models, using the crime of burglary in a middle-class suburb as an illustrative example. These models were, thus, viewed by Clarke and Cornish as potential "blueprints" for theory development by other researchers. Indeed, recognizing that the configuration of such models would differ according to the type of crime under consideration, they simply viewed these models as "good enough" for the early stages of theory formulation. It is in this spirit that we draw on the work of Clark and Cornish in our manuscript.

Of specific relevance to our essay is the initial involvement model (see Figure 3). The model depicts the two key decision points: boxes seven (readiness) and eight (decision to commit a crime). As the model indicates, if an individual becomes motivated and decides that future criminal actions are the best way to satisfy his or her needs (box 3), then the individual will have reached a state of readiness (box 7).

This readiness implies that an individual has evaluated solutions (box 4) to these needs and identified the best course of action (box 5). Such appraisals are further influenced by an individual's moral code, self-perception, and experience of crime as well as the extent to which he or she can plan and employ foresight (box 2). Related to these influences are what Clarke and Cornish called "background factors" (box 1), which customarily have formed the focus for criminological dispositional theories of criminality. Such theories provide accounts of how and why individuals—through the assimilation of specific social or psychological influences or the inheritance of traits—are more inclined to commit delinquent or criminal acts. It is only after an individual has become

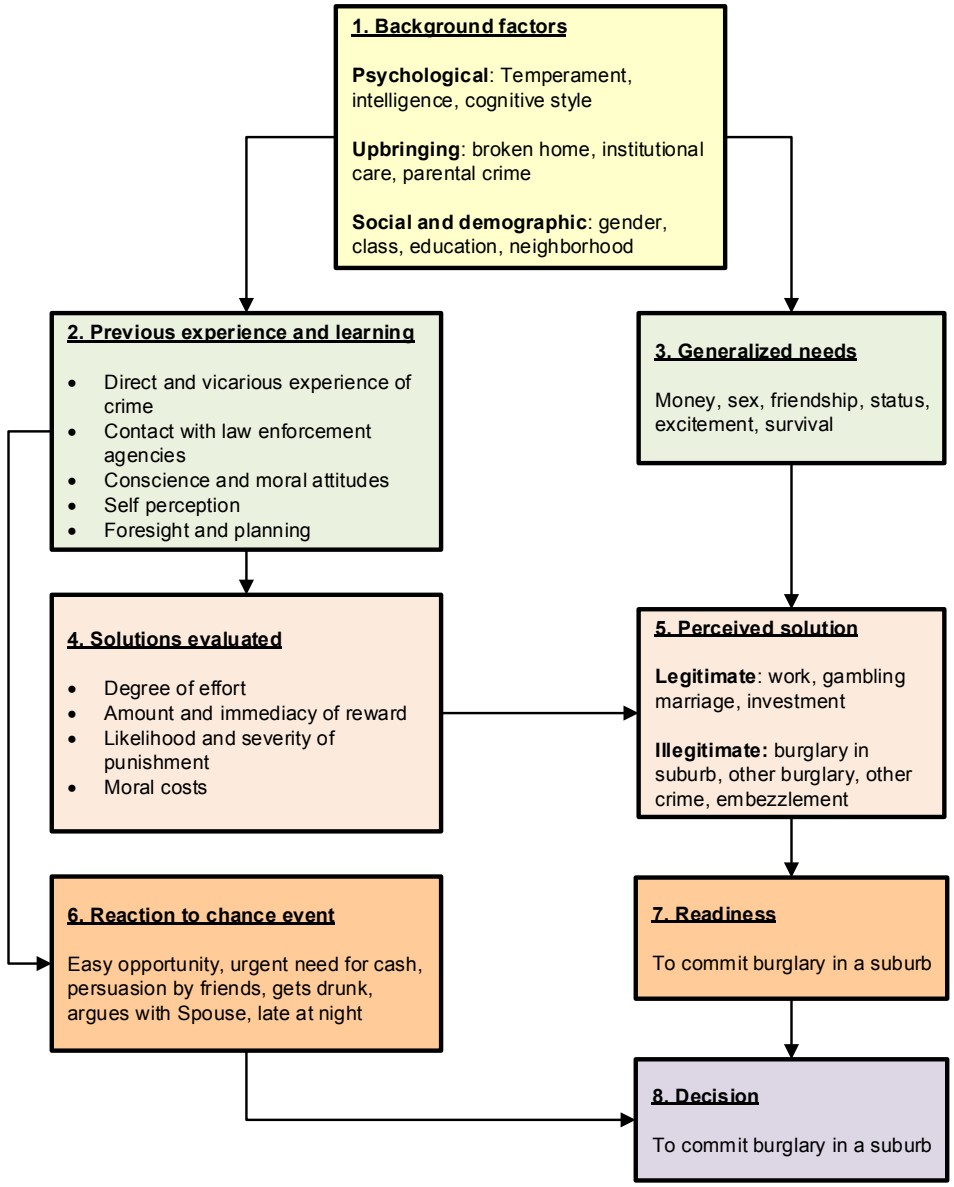

Figure 3. The Initial Criminal Involvement Model, adapted from Clarke and Cornish (1985)

"readied" that the individual will later decide to undertake a specific crime (box 8), which will be influenced by chance events (box 6).

Importantly, the decision to commit a specific crime (box 8) relates to the event stage of the criminal decision-making process, which Clarke and Cornish depicted as a separate diagram. The event stage involves decisions and behavior regarding the actual criminal act.

Based on the distinction between the *initial involvement* and the *event* stage in offender decision making, we now introduce our revised version of the ESAC (Figure 4). We call this revision the Two-Stage Decision-Making Process for ICA. Importantly, Figure 4 reflects the distinction

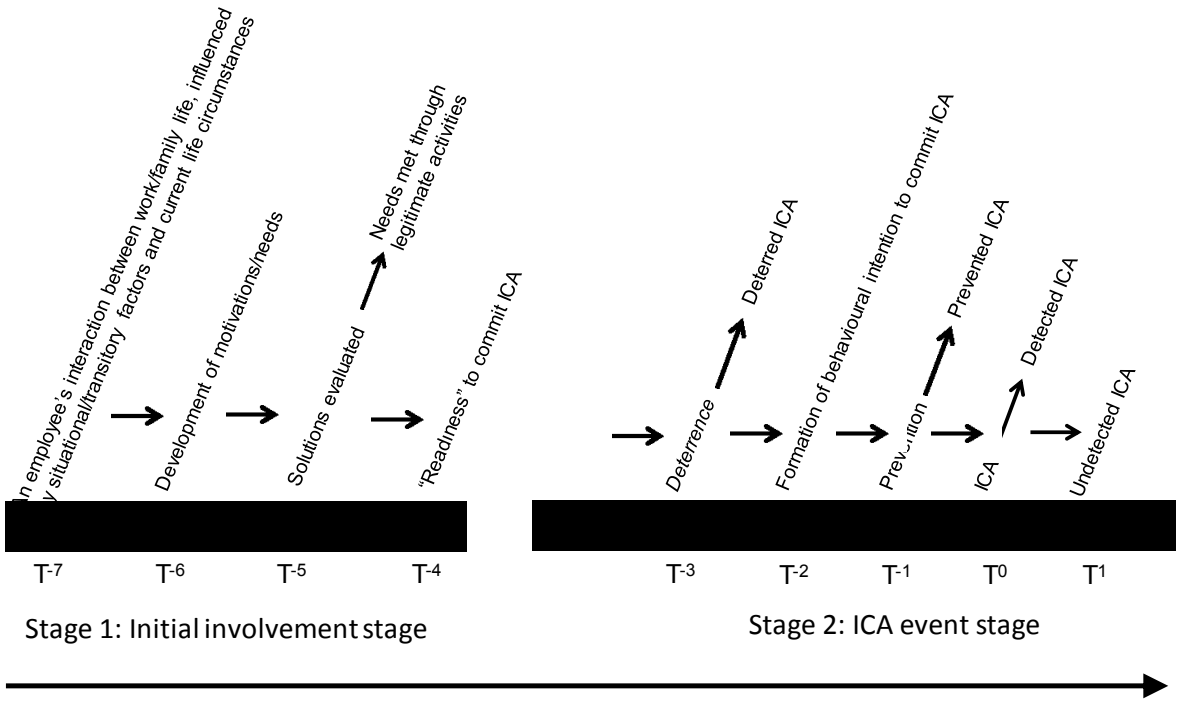

Figure 4. The Two-Stage Decision-Making Process for ICA

between *initial involvement* and what we have termed the *ICA event* stage. Regarding the latter, and working backwards, T^1 represents undetected abuse. T^0 represents the moment when an insider commits actual ICA. Studies that have examined behavioral commission of ICA are uncommon, but a few do exist (Lee et al., 2004a; Lowry et al., 2014; Posey et al., 2011; Workman, 2007). T^{-1} involves attempts to avert ICA, known as *prevention*. Technical approaches to preventing ICA include system and network monitoring, passwords, authentication, and facility control. Few behavioral studies have addressed prevention approaches, with a few notable exceptions (e.g., Willison, 2006; Willison & Backhouse, 2006; Willison & Siponen, 2009). T^{-2} addresses behavioral intentions to commit ICA, and T^{-3} addresses actions to deter negative intentions from forming; such actions are known as *deterrence*. Some studies have researched the interplay between T^{-2} behavioral intentions and T^{-3} deterrence actions (Harrington, 1996; Hu et al., 2011; Peace et al., 2003).

Given this discussion, the point at which the individual reaches a state of *readiness* precedes event deterrence (T^{-4}). However, the state of readiness (T^{-4}) is reached ***only*** if an individual decides that crime is the most suitable course of action, as opposed to the individual's needs being met

through legitimate, non-criminal activities (T^{-5}). The individual must be driven to the point that he or she decides illegitimate activities are the best course of action. To be in a state to make such a decision, an individual must have developed motivations/needs (T^{-6}), which further emerges because of the interactions represented by T^{-7}: An employee's interaction between work and family life, influenced by situational/transitory factors and current life circumstances. The reasons for this specific wording representing T^{-7} and how it leads an individual to T^{-6} are discussed in the following two sections of this manuscript.

4. WHICH FACTORS MOTIVATE INDIVIDUALS TO A STATE OF READINESS FOR ICA?

Given the crucial distinction between the initial involvement and event stages, it is fundamental that IS security research should consider the specific factors that motivate individuals at the initial involvement stage of ICA (see T^{-7} and T^{-6} per Figure 4). In the field of criminology, dispositional theories traditionally have been advanced to explain initial involvement in crime, as Clarke and Cornish (1985) acknowledge (see Figure 3). These theories describe a number of what they term *background factors* (see box 1 in Figure 3). Developed to explain how delinquents and other street criminals first choose to participate in crime, dispositional theories provide accounts of *how* and *why* individuals are more inclined to engage in acts of a delinquent or criminal nature (Agnew, 1992; Cloward & Ohlin, 2013; Hirschi, 2002). These inclinations towards crime emerge through the assimilation of specific social factors (e.g., poor housing, low-quality education, single parents); psychological influences (e.g., mental illness); or the inheritance of traits (e.g., low self-control). However, Clarke and Cornish also noted that the extent to which these background factors are influential—and therefore the extent to which dispositional theories can help to explain initial involvement—depends on the type of crime. Notably, they provided the example of computer fraud as a case in point, arguing that background factors may be much less influential than the individual's immediate situation (Clarke & Cornish, 1985, p. 167):

> *"The contribution of background factors to the final decision to commit crime would be much moderated by situational and transitory influences: and for certain sorts of crime (e.g., computer fraud), the individual's background might be of much less relevance than his*

immediate situation."

The influence of situational and transitory factors on the motivations of individuals is also consistent with white-collar crime research. Unlike delinquent behavior, in which initial involvement in crime occurs early in life or during but not after adolescence (Blumstein, 1986; Piquero & Benson, 2004b), the initial involvement for white-collar criminals generally occurs much later in life. Indeed, studies by Benson and Kerley (2000) and Weisburd and Waring (2001) found the average age at initial involvement for white-collar criminals to be around 40 years old. In an attempt to provide an explanation for this interesting phenomenon, Piquero and Benson (2004b), drew on the findings of existing research (Weisburd, 1991; Weisburd & Waring, 2001; Wheeler et al., 1988) and noted the role of situational influences. Specifically, they highlighted the potential of a crisis in an individual's personal or occupational life that could influence the involvement in offending. This position is supported by earlier white-collar crime research, which emphasized a focus on the current life experiences of individuals for understanding motivational factors. Benson and Kerley (2000, p. 133) clarified these points, as follows:

> *"One searches in vain for early precursors or early hints of trouble in the life-history of the typical white-collar offender. For most of these individuals, their offences appear to come out of nowhere. Their crimes do not appear to be part of longstanding patterns of anti-social conduct, nor do they appear to be deeply rooted in a troubled social background … White collar crime appears to be more a function of adult life experiences as opposed to latent personality traits or a disturbed social background."*

These observations are mirrored in an ever-increasing body of ICA research undertaken by the U.S. Secret Service together with the CERT Division based at Carnegie Mellon University. This research does not emphasize troubled histories of offenders or broken homes but rather focuses on current and situationally specific triggers that lead employees into crime. These groups have conducted a series of studies that highlight how an employee's relationship with his or her organization can often provoke ICA. For example, a 2005 CERT report studied 49 cases of insider sabotage, and in 88% of the cases, the perpetrator held a work-related grievance (Keeney et al., 2005). In addition, various CERT reports have indicated how problems in one sphere of a person's life could influence another. In a report involving the banking and finance sector, for example, the CERT

Division examined 23 ICA cases and found that in 27% of them, individuals were experiencing financial difficulties in their personal lives (Cappelli et al., 2004). Cappelli et al. (2012) offered additional examples, highlighting the role of *internal stressors* (e.g., the threat of layoffs, disagreements over salary) and *external stressors* (e.g., family member with health problems, personal debt) in motivating ICA.

Further evidence has also pointed to "transitory" forces, as noted by Clarke and Cornish (1985), and the need to consider how work/social life domains interact within the context of macro socio-economic forces. Transitory economic recessions can place financial pressures on families and businesses alike. For example, results from a PricewaterhouseCoopers survey indicated that levels of ICA may reflect the current economic climate (PwC, 2012). Specifically, it emphasized that organizational data may be more at risk because of company lay-offs. When the same survey was conducted in 2009, 34% of European respondents believed that risks to company data had increased as a consequence of job losses. By 2011, this figure had risen to 42%. These figures are also echoed in a report by Ernst & Young (2010), in which findings from a survey undertaken in 2009, a year after the emergence of the worldwide credit crunch, revealed that 25% of respondents had witnessed an increased in ICA.

Again, for street criminals, dispositional theories have been developed for explaining their initial involvement in crime. Such theories advance various causes, which are summarized by Clarke and Cornish (1985) as background factors (see Figure 3, box 1). However, Clarke and Cornish also noted that for certain types of crime, including what they termed "computer fraud," these background factors may have far less influence when compared with an individual's immediate situation. Indeed, this section, has illustrated how situational and transitory forces can be seen to originate from the related personal and occupational spheres which can be further influenced by macro socio-economic forces. This points to a considerably more complex picture of the potential motivations for ICA than has previously been considered in the IS security research. This then begs the question as to how such factors should be identified and understood? The next section outlines such an approach.

5. CONSIDERING THE INITIAL INVOLVEMENT FOR ICA THROUGH THE LCP

Here, we propose the application of the LCP (Elder, 1994, 1998) to clarify the ICA motivational influences (located in box 1 of Figure 3; see also T^{-7} and T^{-6} per Figure 4) at the initial involvement stage. The LCP has its origins in sociology but has extended its reach to other disciplines, including social history (Modell, 1989), developmental psychology (Bronfenbrenner, 1979), and gerontology (Streib & Binstock, 1990). The LCP represents a substantial change in the study of people and their lives. Central to this examination is a focus on *time*, *context*, and *process*. LCP traditionally has considered three trajectories in individuals' lives: their education, work, and family. LCP research has studied the interdependency of these trajectories while considering how development in these trajectories is affected by historical/socio-economic forces and short-term transitions. These transitions (or "events") can include factors such as commencing university studies, changing jobs, becoming unemployed, getting married, having a child, getting divorced, and experiencing bereavement from death of a loved one.

Crucially, LCP is not a theory, but rather a perspective that can help conceptualize and study phenomena. Thus, Elder (1998) noted that the *life course* "defines a common field of inquiry by providing a framework that guides research on matters of problem identification and conceptual development" (p. 4). As depicted in Figure 5, four key principles form the framework advanced by Giele and Elder (1998): (1) time and place, (2) timing, (3) linked lives, and (4) human agency. We advance this framework as the basis for providing insights into the contemporary, transitory, and situational factors that motivate an individual to initial involvement in criminal behavior. We note how the relationship among the three trajectories of education, work, and family and contemporary, transitory, and situational factors can lead an individual into a fourth trajectory—crime.

Next, we discuss each of the four principles and provide illustrations of their applications in LCP research. Given the absence of IS security research focusing on the factors that influence initial involvement in ICA, we also draw on white-collar crime research as a means to illustrate how the framework could be applied to the IS security field. One major advantage of applying the LCP framework to IS security research is that it provides a lens through which to conceptualize influential

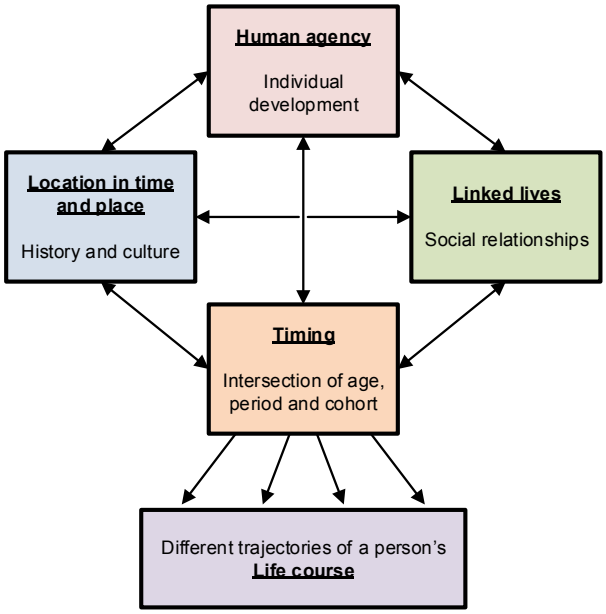

Figure 5. Four Key Principles in the LCP Framework, adapted from Giele and Elder (1998)

factors and understand the relationships amongst them, just as applied to white-collar crime.

We justify the use of the white-collar crime literature by arguing that the line between white-collar crime and ICA is increasingly blurred. This blurring is due to the proliferation of computers and their use by white-collar employees. A similar argument is provided by Weisburd and Waring (2001, p. 11) who note:

> *"[C]hanges in our society … have placed the opportunity for white-collar crimes in the hands of a much broader class of Americans, most of them who were excluded from these activities in the past. In part, the rapid growth of white-collar jobs in America in the last fifty years had spawned such changes (Bell, 1973). But perhaps even more important are the dramatic differences in the way modern society functions. The advent of the computer, for example, gives large numbers of people access to the documents and transactions that are so much a part of white-collar illegalities."*

5.1 Principal One: Time and Place

The principle of *time and place* states that "the life course of individuals is embedded in and shaped by the historical times and places they experience over their lifetime" (Elder, 1998, p. 3). Differences in when individuals are born exposes them to varied historical worlds. These worlds offer both constraints and opportunities, which are reflected in the individuals' lives. The influences of specific historical times and places on people take the form of a *cohort effect*, in which successive cohorts reflect the historical epochs through which they live. An example of this principle is provided

by Zhou and Hou (1999), who studied the effects of the Chinese Cultural Revolution (1966–1976) on Chinese youth. During this period, a large number of Chinese youths experienced being "sent down," a process that involved separation from their families and communities and being forced to undertake manual labor. Such an experience had a profound effect on the life course of these youths and differentiated this specific cohort from successive groups that did not experience the same fate.

The principal of *time and place* provides insight into how influential factors may emerge depending on the historical epoch. This principle has been illustrated in recent years with that widespread organizational lay-offs, resulting from the recent global downturn. The influence of macro socio-economic forces also has been discussed in a series of white-collar crime studies (Benson & Moore, 1992; Wheeler, 1992). Indeed, Benson and Moore (1992) argued that during economic prosperity, an ever-present opportunity for an employee to embezzle may remain just that—an opportunity. However, a recession may influence the employee to consider crime to make ends meet. For example, his or her partner may become unemployed, forcing a reinterpretation of the opportunity and the enactment of embezzlement. Accordingly, Benson and Moore concluded that any theory of white-collar crime must consider macro socio-economic forces due to their potential to influence initial involvement in crime.

5.2 Principle Two: Timing

The second principle of *timing* states that "the developmental impact of a succession of life transitions or events is contingent on when they occur in a person's life" (Elder, 1987, p. 3). The study by Elder (1987) of men from Oakland, California, who were mobilized to fight in World War II, provides an illustration of this principle. The study found that the effect of mobilization depended on the men's life stage. For instance, *early entrants*—those who entered the military before they were 21 years old—experienced little disruption in their life course. Of this group, few were married or in a steady relationship when mobilized. For *late entrants*—those who entered the military at ages 22 or older—the picture was far different. These men were three times as likely to be living with a wife compared with the early entrants. Late army entrants also experienced greater disruption regarding work. Many of these men already had established a career prior to being called up, which was not the

case for early entrants. Indeed, many of the early entrants used the opportunities offered by the G.I. Bill, post-war, to enter college and then establish a career.

In the organizational domain, the principle of timing can be illustrated by examining the relationship between threats to an employee's job security (Kinnunen et al., 1999; Sverke & Hellgren, 2002) and the employee's life stage. As time passes, an employee's identity may change to that of breadwinner (Thébaud, 2010; Warren, 2007). A breadwinner is likely to accrue additional financial responsibilities in the form of a mortgage, new car, child care, and schooling fees. In her study of ICT workers, Kelan (2008) noted how the extra financial burden breadwinners experience led to them to place a greater emphasis on job security. However, job security was not such a priority for unmarried individuals who had no children and, therefore, fewer financial responsibilities. Parallels can be drawn here with the work of Charles and James (2003), who studied the relationship between job insecurity and work orientations for men and women. Based on interviews with staff from three different employment sectors (manufacturing, public, retail), they noted that the significance of paid work for each respondent affected their attitudes towards job security. Highlighting the importance of employment stability, for example, one respondent stated the following (p. 252):

> *"When I was single, when I first started here I was single, it didn't matter to me if this place closed or not. Because I had no dependents. I didn't have to— there was just myself I was taking care of. And when you get married and you get a house and you have got a mortgage and a couple of kids come along—that's the difference."*

This research illustrated that employees react differently to a firm's financial problems and the ensuing threats to job security. Notably, these reactions depend on their life stages and their marital/familial responsibilities. In extreme cases, in a bid to ensure the family's financial stability, a breadwinner may resort to ICA. Supporting evidence for this assertion comes from studies in which convicted white-collar offenders were interviewed about the motives for their offenses (Klenowski et al., 2011; Willot et al., 2001). In the study by Willot et al. (2001), for example, four offenders described as upper-middle class discussed not only their own financial responsibilities, but also those of the employees who worked for them. This factor is illustrated in the following excerpt from an offenders' group discussion (p. 450):

> ***Francis****: If it had just been me, I don't think … there would probably have been no need, to, to have to dig into these funds because …*
>
> ***Lawrence****: I agree, if I was a single person, I would just have walked away, it wouldn't have concerned one.*
>
> ***Rupert****: Yeah, I think that is a strong factor, because although my family's grown up now, at the time this happened, I had a young family. Then you look to your staff, who in turn have got their responsibilities and young families themselves.*

5.3 Principle Three: Linked Lives

The third principle of *linked lives* asserts that "lives are lived interdependently, and social and historical influences are expressed through this network of shared relationships" (Elder, 1998, p. 4). Of some significance, these shared relationships are not trajectory specific but rather cross the boundaries of education, work, and family life. The fact that these relationships are not trajectory specific enables consideration of how these areas of life can influence each other. Drawing on this principle, Bailey et al. (2004) conducted a grounded theory study which explored how dual-earner households make decisions about migration with respect to home and work tasks. Specifically, in terms of home tasks, they looked at how couples manage their caring responsibilities for their own children and elderly parents. Bailey *et al.* noted the following (p. 1628):

> *"What emerges, then, is the view that (im)mobility is influenced by how household networks trigger, enable and constrain migration, and that the strength of these networks over space and time affects the balance of enabling and constraining factors. When local linkages are not strong, families move to be near parents, even if this requires adjustments to employment careers. However, when local linkages are strong, elderly parents are moved to be near their children."*

The breadwinner example also helps to demonstrate the principle of linked-lives in that the LCP affords consideration of how the spheres of work and personal life may influence each other. With the case of the breadwinner, it is clear how changes in an employee's personal life may affect decisions in the work environment. Wheeler (1992) provides another example, noting how white-collar criminals are not always driven by the desire for more; rather, they often seek simply to maintain what they have. Speculating in a previous study, Weisburd (1991, p. 189) noted, …

> *"[certain potential offenders] would be reasonably happy with the place they have achieved through conventional means if only they could keep that place. But the fate of organizational success and failure, or the changing nature of the economy in their line of work may put them at least temporarily under great financial pressure, where they risk losing the lifestyle that*

> *they have achieved. They may perceive this situation as a short-term threat that can be met through short-term fraud—a temporary taking to be restored as soon as their business fortunes turn around. The motivation for their crime is not selfish ego gratification, but rather the fear of falling—of losing what they have worked so hard to gain."*

Wheeler's argument is supported by a number of self-report studies, which have found that the motive for white-collar crime is sometimes the desire to maintain what has been achieved through hard work as opposed to greed and the desire for more (Benson, 1985; Denzin, 1977). Rothman and Gandossy (1982), for instance, provided an example of a man who co-owned a building business with his brothers. He preferring to leave the bookkeeping to his siblings; then one day they informed him that it had been essential to commit white-collar crime offenses to keep their company afloat. Although shocked and angered by the news, the man did not report his brothers' actions. Rather, concerned about the economic welfare of his family, he decided that complicity was the best course of action.

5.4 Principle Four: Human Agency

The fourth and final LCP principle is that of *human agency*. This principle states that "individuals construct their own life course through the choices and actions they take within the opportunities and constraints of history and social circumstances" (Elder, 1998, p. 4). Gong et al. (2011) examined this principle in terms of how human agency can influence the relationship between migration and mental health. Specifically, they studied human agency in terms of the reasons for migration, the extent to which the migration was planned, and whether the migration was voluntary or involuntary (e.g., a refugee fleeing from war and seeking political asylum). Of particular interest to the researchers was the extent to which the exercise of human agency before migration influenced the mental well-being of the migrants once they had moved and were attempting to adapt to their new country of residence. Using a sample of Asian immigrants who migrated to the US between 2002 and 2003, the study produced two major findings. First, individuals who had a number of strong reasons to move were less likely to experience mental health problems compared with those who lacked a clear rationale. Secondly, there were psychological benefits for those who carefully planned their migration. Gong et al. (2011) argued that planning—the accumulation of financial resources,

acquiring language training, and establishing new social networks—lessened the distress of the move and reduced the likelihood of mental disorders.

The principle of human agency appears well suited to a discussion of white-collar crime in which offenders and potential offenders are considered rational decision makers (Benson & Cullen, 1988; Weisburd et al., 1995). In addition, white-collar crime research has noted how social circumstances are influenced by historical socio-economic forces; that is, such influences may be present in one period but not in others. As discussed, Benson and Moore (1992) argued that any theory of white-collar crime must consider macro social and economic forces due to their influence on the decision-making process of offenders. They asserted that when an economy is buoyant, an employee may be aware of an ever-present embezzlement opportunity, but it may remain simply a notion or passing temptation. However, a recession could influence the employee's firm negatively, threatening the employee's job security and forcing him or her to reconsider the embezzlement opportunity.

Aside from the arguments made by Benson and Moore (1992), several other studies of offender accounts have highlighted the influence of historical and social circumstances and their influence on the decision making of white-collar criminals (e.g., Benson, 1985; Klenowski et al., 2011; Rothman & Gandossy, 1982). In keeping with our discussion of breadwinning (see Principle Two: Timing), Klenowski et al. (2011) studied the accounts of men and women who were convicted of white collar offenses. One offender, named Xavier, made the following argument (p. 55):

> *"I guess when I was committing my acts, I believed that maybe I was doing some of this for my family. I wanted to have the time and the financial security to be around my family to make sure that I would be there for my children, so I guess family also subconsciously played into why I did what I did. It all boils down to power and greed and decisions you make in life; in my case, my family was part of my decision making for why I did what I did*."

6. THE FUTURE OF ICA RESEARCH

Although ICA remains a major threat for businesses, as noted, the response from IS security researchers has been relatively modest. Nonetheless, recent IS security research has urged a greater focus on the insider threat (Crossler et al., 2013; Mahmood et al., 2010; Posey et al., 2013; Warkentin & Willison, 2009; Willison & Warkentin, 2013), the vast bulk of this research is focused on policy

noncompliance with noncriminal violations (e.g., Barlow et al., 2013; Boss et al., 2015; Cheng et al., 2013; D'Arcy & Devaraj, 2012; Guo & Yuan, 2012; Guo et al., 2011; Hsu et al., 2015; Johnston et al., 2015; Posey et al., 2015; Siponen & Vance, 2010; Vance et al., 2015). Although noncriminal behaviors are indeed important to study, criminal behaviors can be particularly damaging to organizations and thus need greater focus in the literature. In a bid to address the need for more and better ICA research, this paper encompasses two aims: to demonstrate a gap in the IS security research, via the RCP, and to introduce the LCP for studying the motivations for ICA. First, it is clear the research has focused almost solely on factors influencing an individual's decision regarding intentions for ICA. However, such research has overlooked another key stage in the criminal decision-making process: Through the application of the RCP, we illustrate how existing research on ICA has failed to consider those motivational factors that could lead to initial involvement and a state of readiness. This omission has led us to advance a revised version of the ESAC we call the Two-Stage Decision Making Process for ICA. Second, we aim to advance and demonstrate the application of a framework based on the LCP, which can assist researchers in identifying these motivational factors at the initial involvement stage.

As can be seen through a discussion of the four LCP principles, this approach enables a dynamic perspective for considering the motivations that influence the decision to participate in criminal behavior. First, regarding the principle of *time and place*, the perspective affords insight into how influential factors may emerge depending on the historical epoch. Second, the principle of *timing* helps to examine how a specific event may affect individuals differently, depending on their life stage. Third, the principle of *linked-lives* fosters consideration of how the spheres of work and personal life may influence each other. Fourth, the principal of *human agency* encourages understanding of how individuals' life courses are constructed as they make choices about criminal behavior. These choices reflect the current realities and opportunities of historical and social circumstances.

Embracing and integrating the RCP and LCP into IS security research should not only cause a major shift in the theoretical lens that focuses on ICA, but also open up previously hidden avenues of compelling research. We thus conclude by offering further thoughts on what these perspectives should

mean for future research. We first argue that the concepts we have introduced in this essay cannot be waved off as mere covariates of ICA. Next, based on our discussion of the white-collar crime literature in relation to the LCP, we also offer a possible alternative to deterrence theory when considering offender decision making.

6.1 The LCP Requires More Than Mere Covariates

Given the extant trend in IS security research to focus on intentions to commit ICA and to address counter-explanations as covariates, we warn against treating the concepts we have introduced as mere covariates. For example, modelling intentions to commit ICA with demographics of marital status, organization's economic status, and personal financial pressure, does not properly use the LCP. Such factors first need to be explained first in terms of offender readiness, which is a key missing construct in the IS literature that temporally precedes intentions and has unique antecedents; crucially, readiness is not a covariate of intentions. Although hints of these interrelationships can be found in the literature, only the LCP can provide an understanding of how they are related and why. Notably, most current IS security models are cross-sectional in nature and do not consider temporal influences, let alone the crucial missing link of readiness and the life events that encourage readiness. Some may argue that focusing only on intention with its covariates provides theoretical concision; however, we argue that such "concision" misrepresents the reality of ICA. Thus, new models are needed that consider temporal influence of the events leading up to actual ICA.

Complementary to these models, ICA researchers need to expand their methodological and measurement repertoire to study these phenomena. The current common practice of using one-off surveys or hypothetical vignettes are likely to come up short in effectively studying our two-stage event-based model. We thus believe it is crucial that ICA researchers turn to longitudinal data collections or our proposed timeline of events cannot be properly studied or measured in a causal manner. To do so, ICA researchers will likely need to follow truly longitudinal event studies conducted in Sociology and in Criminology, which often take place over years, not months. In doing so, greater care needs to be taken for triangulating measurement with actual events rather than solely relying on participating self-report. Such studies would definitely need to involve participants (i.e.,

employees) responding to questions about life events and their ICA behaviors, but for improved data, manager reports on the employees' behaviors would also be needed.

Another promising avenue of research would be to better leverage big-data analytics methods to better understand life events and organizational events that might act as triggers that foster motivations and readiness to commit ICA. Although there would be ethical concerns with such research and practice that would need to be carefully addressed, organizations have already legal used predictive analytics on their employees to predict factors such as who is most likely to leave their employment prematurely. Organizations would not be privy to all key life events that could trigger ICA, but they are legally privy to some that could be studied in a consistent, predictive manner (e.g., change in marital status, surviving a round of layoffs in a department, credit score changes, change in number of family dependents, poor work reviews).

6.2 Advancing RCP and LCP for understanding offender decision making at the event stage.

Here, we urge IS security researchers to look beyond intentions and consider the decision making and actual behaviors involved in the perpetration of ICA. As noted, intention is often used a proxy for behavior, but we argue that this leads to misplaced assumptions about the ICA commission process, which belie its complexity. Although we have concentrated on the motivations for ICA at the "initial involvement" stage, we also propose that the LCP and RCP can provide much needed clarity in terms of what to research at the "event" stage by examining opportunities for ICA. We discuss these next.

In discussing white-collar crimes, Piquero and Benson (2004a) argued that offences may be "situationally dependent" on two levels. First, and consistent with our arguments, they noted that an individual may experience a crisis in their work or personal life that motivates the commission of a white-collar crime (e.g., financial strain due to bankruptcy or divorce). However, they also noted that white collar-offending may be situationally dependent in the sense that the opportunity to offend may not come about until they have secured a certain occupational position. They emphasized that, unlike street offenders, the opportunities for white-collar criminals, are not ubiquitous or so democratically distributed. Rather, access to opportunities are shaped by the occupational position undertaken by an

employee and the structure of the organization in which an employee works.

As illustration, an accountant may perceive an opportunity for embezzlement, which can be executed through the use of his/her company's online book-keeping system. Due to his/her access to and knowledge of the book-keeping system, which arose from the nature of his/her position, the accountant may perceive an embezzlement opportunity; yet, it is unlikely that a marketing employee from the same company would equally view the booking-keeping system as offering them an opportunity for embezzlement. Given his/her different position, the marketing employee would likely not have access to the company accounts or know how to use the online book-keeping software. In this sense, organizations play an important role in shaping what is termed the *opportunity structure* — that is, how a specific context may offer/deny opportunities, depending on the individual.

When considering these two aspects of situational dependency in terms of the LCP, the latter may also help to explain why white-collar and ICA offenders commit their offences at a later stage of their life course, when compared with juvenile delinquents or street offenders. A key point is that the LCP affords consideration of the inter-play between trajectories and how events in one may have implications for another and lead to the "initial involvement" in crime. Previously law abiding individuals who have assimilated the trappings and behaviors of the middle-class may be following conventional trajectories in their work and family life. Many such individuals may have academic degrees and worked hard to attain their occupational positions. Achieving these goals takes time and represent periods of conformity to general society. Yet a crisis in their work or family life, may lead them to consider crime as a solution to their newly developed needs. Given the previous conventional course of the trajectories followed by such individuals, this leads them to resorting to crime at a much later stage in their life, when compared with juvenile delinquents, who will commence criminal activities in their teenage years. Therefore, without consideration of the inter-play between the different life course trajectories, it is difficult to conceptualize the factors which lead to the "initial involvement" and later the perpetration of white-collar/ICA offenses in the "event" stage.

The manner in which the environment shapes potential opportunities is also consistent with the RCP. Regarding their "initial involvement" model, Clarke and Cornish argued that if an offender

decides that criminal actions are the best means through which to satisfy their needs, then they will have reached a state of "readiness." Therefore, it is only *after* an individual has reached this state, that, at a later date, they will select an opportunity and perpetrate a specific crime in the "event" stage. Such opportunities will be selected based on the associated costs and benefits. Notably, the RCP adopts a crime-specific approach for understanding why certain opportunities are acted on and not others. To help elucidate the factors that an offender considers when undertaking this cost-benefit analysis, Cornish and Clarke (1987) advanced the concept of "choice-structuring" properties. Such properties relate to not only the offense, but also the offender. Therefore, in terms of specific offenses, factors can include the type of crime, type and amount of "payoff," perceived risk, skills required, and so on. These in turn will be considered by the offender regarding their own goals, motives, experiences, abilities, expertise and preferences. Given the nature of the relationship between offense and offender, choice structuring properties helps to explain the basis on which opportunities are selected and why certain offenses will be differentially attractive to some offenders and not others. There is a notable overlap here with Piquero and Benson (2004a) who noted the importance of how organizations play a role in "structuring" opportunities for potential offenders, but Cornish and Clarke (1987, p. 943) take this one step further, by also highlighting the choice-structuring properties of the individual:

> *. . .the term "choice-structuring property" is a relational concept designed to provide an analytic tool for increasing an understanding of the interaction between person variables and arrays of behaviors – in the case of crime, to specify more closely offenders as well as the offenses they commit.*

The above insights from the LCP and RCP emphasize the complexity of the commission process and the close relationship between offender and offense. It is clear that a focus on behavior in the commission process is required. A continued focus on intention, without an appreciation of how an offence is chosen, will perpetuate a myopic understanding of the problem.

7. CONCLUSION

In this manuscript, we challenge the existing body of research in criminal organizational (ICA), which we assert has too narrowly focused on factors that influence either ICA intentions or actual behavior

during the commission process. The key opportunity is that this literature is missing is that ICA research has failed to correctly conceptualize, and subsequently measure or test, the decision-making processes involved in ICA. We demonstrate this deficiency by leveraging the RCP from criminology, which newly introduced the idea of an "initial involvement" stage, which encompasses those factors that lead an individual to consider participation in ICA. Importantly, RCP argues that if, during the initial involvement stage, an individual becomes motivated and decides that future ICA behavior is the most suitable course of action, then he or she will have reached a state of "readiness." It is only after an individual has become readied, and at a later time, does the individual make event decisions in the perpetration of a specific crime. As the extant research has not considered the initial involvement stage, or the idea of "readiness," we propose a revised version of the ESAC, which reflects these criminal decision-making stages.

Another contribution of our work is to further consider what exactly happens to people that would create motivations or needs that would lead to readiness. Again, the ICA is silent on these motivational triggers. Accordingly, we draw on the LCP. With a focus on time, context, and process, the LCP offers a framework in which are inscribed four key principles. Through the LCP, we can better understand why white collar crimes such ICA often occur later in one's life. For example, it might require a key event such as financial strain during an ugly divorce, with a combination of one's access to opportunities through their work position (e.g., system authorization that could allow for embezzlement) that provide motivation that leads to readiness. Through examples drawn from the LCP and white-collar crime literature, we illustrate how these principles can provide a basis for conceptualizing factors that motivate ICA and open up new avenues for future research/theory development. We conclude by providing an outline of exciting research opportunities based on the RCP and LCP.

REFERENCES

Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. *Criminology, 30*(1), 47-88.

Anonymous (2015). US cybersecurity: Progress stalled: Key findings from the 2015 US State of Cybercrime Survey. Retrieved from http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf

Bachmann, M. (2010). The risk propensity and rationality of computer hackers. *International Journal of Cyber Criminology, 4*(1&2), 643-656.

Bailey, A., Blake, M., and Cooke, T. (2004). Migration, care, and the linked lives of dual-earner households. *Environment and Planning A, 36*(9), 1617-1632.

Barlow, J. B., Warkentin, M., Ormond, D., and Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security, forthcoming*.

Benson, M. L. (1985). Denying the guilty mind: Accounting for involvement in a white-collar crime. *Criminology, 23*(4), 583-607.

Benson, M. L. and Cullen, F. T. (1988). The special sensitivity of white-collar offenders to prison: a critique and research agenda. *Journal of Criminal Justice, 16*(3), 207-215.

Benson, M. L. and Kerley, K. R. (2000). Life course theory and white-collar crime. In H. Pontell & D. Shichor (Eds.), *Contemporary Issues in Crime and Criminal Justice: Essays in Honor of Gilbert Geis* (pp. 121-136). Upper Saddle River, New Jersey: Prentice Hall.

Benson, M. L. and Moore, E. (1992). Are white-collar and common offenders the same? An empirical and theoretical critique of a recently proposed general theory of crime. *Journal of Research in Crime and Delinquency, 29*(3), 251-272.

Blumstein, A. (1986). *Criminal Careers and 'Career Criminals'* (Vol. 2). Washington, DC: National Research Council.

Blumstein, A., Cohen, J., and Farrington, D. P. (1988). Criminal career research: Its value for criminology*. *Criminology, 26*(1), 1-35.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. (2015). What do users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly, 39*(4), 837-864.

Bossler, A. M. and Burrus, G. W. (2011). The general theory of crime and computer hacking: Low self-control hackers. In T. J. Holt & B. H. Schell (Eds.), *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (pp. 38-67). Hershey, Pennsylvania: Information Science Reference.

Bronfenbrenner, U. (1979). *The Ecology of Human Development*. Cambridge, Massachusetts: Harvard University Press.

Cappelli, D., Keeney, M., Kowalski, E., Moore, A., and Randazzo, M. (2004). Insider threat study: Illicit cyber activity in the banking and finance sector. Retrieved from http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=50287

Cappelli, D. M., Moore, A., and Trzeciak, R. (2012). *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*. Boston, Massachusetts: Addison-Wesley Professional.

Charles, N. and James, E. (2003). Gender and work orientations in conditions of job insecurity. *The British Journal of Sociology, 54*(2), 239-257.

Cheng, L., Li, Y., Li, W., Holm, E., and Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security, 39, Part B*(0), 447-459.

Clarke, R. and Cornish, D. (1985). Modelling offender's decisions: A framework for policy and research. In M. Tonry & N. Morris (Eds.), *Crime and Justice: An Annual Review of Research (Vol. 6)* (pp. 147-185). Chicago, Illinois: University of Chicago Press.

Cloward, R. A. and Ohlin, L. E. (2013). *Delinquency and Opportunity: A Study of Delinquent Gangs* (Vol. 6). New York, New York: Routledge.

Cornish, D. and Clarke, R. (1987). Understanding crime displacement: An application of rational choice theory. *Criminology, 25*(4), 933-947.

Cornish, D. B. and Clarke, R. V. (2013). Introduction. In D. Cornish & R.Clarke (Eds.), *The Reasoning Criminal: Rational Choice Perspectives on Offending* (pp. 1-16). New York, New York: Transaction.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*(February), 90-101.

Cummings, A., Lewellen, T., McIntire, D., Moore, A., and Trzeciak, R. (2012). Insider threat study: Illicit cyber activity involving fraud in the U.S. financial services sector. *Special Report CMU/SEI-2012-SR-004, 2012*. Retrieved from http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=27971#

D'Arcy, J. and Devaraj, S. (2012). Employee misuse of information technology resources: Testing a contemporary deterrence model. *Decision Sciences, 43*(6), 1091-1124.

D'Arcy, J. and Hovav, A. (2007). Deterring internal information systems misuse. *Communications of the ACM, 50*(10), 113-117.

D'Arcy, J. and Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics, 89*(1), 59-71.

D'Arcy, J., Hovav, A., and Galletta, D. (2009a). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79-98.

D'Arcy, J., Hovav, A., and Galletta, D. F. (2009b). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research, 20*(1), 79-98.

Denzin, N. (1977). Notes on the criminogenic hypothesis: a case study of the American liquor industry. *American Sociological Review, 42*(6), 905-920.

Elder, G. (1987). War mobilization and the life course: a cohort of World War II veterans. *Sociological Forum, 2*(3), 449-472.

Elder, G. (1994). Time, human agency, and social change: perspectives on the life course. *Social Psychology Quarterly, 57*(1), 4-15.

Elder, G. (1998). The life course as development theory. *Child Development, 69*(1), 1-12.

Ernst & Young (2010). *12th Annual Global Information Security Survey: Outpacing Change*: Ernst & Young.

Giele, J. and Elder, G. (1998). Life course research: Development of a field. In J. Giele & G. Elder (Eds.), *Methods of Life Course Research: Qualitative and Quantitative Approaches*. Thousand Oaks, California: SAGE.

Gong, F., Xu, J., Fujishiro, K., and Takeuchi, D. T. (2011). A life course perspective on migration and mental health among Asian immigrants: the role of human agency. *Social Science & Medicine, 73*(11), 1618-1626.

Guo, K. H. and Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: a mediating model. *Information & Management, 49*(6), 320-326.

Guo, K. H., Yuan, Y., Archer, N. P., and Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: a composite behavior model. *Journal of Management Information Systems, 28*(2), 203-236.

Hansen, J. V., Lowry, P. B., Meservy, R., and McDonald, D. (2007). Genetic programming for prevention of cyberterrorism through dynamic and evolving intrusion detection. *Decision Support Systems, 43*(4), 1362-1374.

Harrington, S. J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly, 20*(3), 257-278.

Herath, T. and Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 28*(2), 106-125.

Hirschi, T. (2002). *Causes of Delinquency*. New Brunswick, New Jersey: Transaction.

Hovav, A. and D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information & Management, 49*(2), 99-110.

Hsu, J., Shih, S.-P., Hung, Y. W., and Lowry, P. B. (2015). The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research, 26*(2), 282-300.

Hu, Q., Xu, Z., Dinev, T., and Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM, 54*(6), 54-60.

James, T. L., Lowry, P. B., Wallace, L., and Warkentin, M. (2017). The effect of belongingness on

obsessive-compulsive disorder in the use of online social networks. *Journal of Management Information Systems, forthcoming*(doi: http://dx.doi.org/10.1080/07421222.2017.1334496).

Jenkins, J. L., Grimes, M., Proudfoot, J., and Lowry, P. B. (2014). Improving password cybersecurity through inexpensive and minimally invasive means: detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time warnings. *Information Technology for Development, 20*(2), 196-213.

Johnston, A. C., Warkentin, M., and Siponen, M. T. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS quarterly, 39*(1), 113-134.

Keeney, M., Kowalski, E., Cappelli, D., Moore, A., Shimeall, T., and Rogers, S. (2005). Insider threat study: Computer systems sabotage in critical infrastructure sectors. Retrieved from http://www.cert.org/insider_threat/insidercross.html

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., and Greer, C. (2013). Information disclosure on mobile devices: re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies, 71*(12), 1163-1173.

Kelan, E. (2008). Gender, risk and employment insecurity: the masculine breadwinner subtext. *Human Relations, 61*(9), 1171-1202.

Kinnunen, U., Mauno, S., Natti, J., and Happonen, M. (1999). Perceived job insecurity: a longitudinal study among Finnish employees. *European Journal of Work and Organizational Psychology, 8*(2), 243-260.

Klenowski, P., Copes, H., and Mullins, C. (2011). Gender identity, and accounts: how white collar offenders do gender when making sense of their crimes. *Justice Quarterly, 28*(1), 46-69.

Lai, F., Li, D., and Hsieh, C.-T. (2012). Fighting identity theft: the coping perspective. *Decision Support Systems, 52*(2), 353-363.

Lee, S. M., Lee, S. G., and Yoo, S. (2004a). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management, 41*(6), 707-718.

Lee, Z., Lee, Y., and Kim, Y. (2004b). Personal web page usage in organizations. In M. Anandarajan & C. A. Simmers (Eds.), *Personal Web Usage in the Workplace: A Guide to Effective Human Resources Management* (pp. 28-45). Hershey, Pennsylvania: Information Science Publishing.

Loch, K. D., Carr, H. H., and Warkentin, M. E. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly, 16*(2), 173-186.

Lowry, P. B., Posey, C., Bennett, R. J., and Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal, 25*(3), 193-230.

Lowry, P. B., Posey, C., Roberts, T. L., and Bennett, R. J. (2014). Is your banker leaking your personal information? The roles of ethics and individual-level cultural characteristics in predicting organizational computer abuse. *Journal of Business Ethics, 121*(3), 385-401.

Lowry, P. B., Zhang, J., Wang, C., and Siponen, M. (2016). Why do adults engage in cyberbullying on social media? An integration of online disinhibition and deindividuation effects with the social structure and social learning (SSSL) model. *Information Systems Research, 27*(4), 962-986.

Lowry, P. B., Zhang, J., and Wu, T. (2017). Nature or nurture? A meta-analysis of the factors that maximize the prediction of digital piracy by using social cognitive theory as a framework. *Computers in Human Behavior, 68*(March), 104-120.

Mahmood, M. A., Siponen, M., Straub, D., Rao, H. R., and Raghu, T. S. (2010). Moving toward black hat research in information systems security: an editorial introduction to the special issue. *MIS Quarterly, 34*(3), 431-433.

Modell, J. (1989). *Into One's Own: From Youth to Adulthood in the United States 1920-1975*. Berkeley, California: University of California Press.

Moody, G. D. and Siponen, M. (2013). Using the theory of interpersonal behavior to explain non-work-related personal use of the Internet at work. *Information & Management, 50*(6), 322-335.

Moore, R. and McMullan, E. C. (2004). Perceptions of peer-to-peer file sharing among university

students. *Journal of Criminal Justice and Popular Culture, 11*(1), 1-19.
Nandedkar, A. and Midha, V. (2012). It won't happen to me: an assessment of optimism bias in music piracy. *Computers in Human Behavior, 28*(1), 41-48.
Paternoster, R. (1989a). Absolute and restrictive deterrence in a panel of youth: Explaining the onset, persistance/desistance, and frequency of delinquent offending. *Social Problems, 36*(3), 289-309.
Paternoster, R. (1989b). Decisions to participate in and desist from four types of common delinquency: Deterrence and the rational choice perspective. *Law & Society Review, 23*(1), 7-40.
Peace, A. G., Galletta, D. F., and Thong, J. Y. L. (2003). Software piracy in the workplace: A model and empirical test. *Journal of Management Information Systems, 20*(1), 153-177.
Piquero, N. and Benson, M. (2004a). White-collar crime and criminal careers: Specifying a trajectory of punctuated situational offending. *Journal of Contemporary Criminal Justice, 20*(2), 148-165.
Piquero, N. L. and Benson, M. L. (2004b). White-collar crime and criminal careers specifying a trajectory of punctuated situational offending. *Journal of Contemporary Criminal Justice, 20*(2), 148-165.
Posey, C., Bennett, R. J., Roberts, T. L., and Lowry, P. B. (2011). When computer monitoring backfires: invasion of privacy and organizational injustice as precursors to computer abuse. *Journal of Information System Security, 7*(1), 24-47.
Posey, C., Roberts, T. L., and Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems, 32*(4), 179-214.
Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., and Courtney, J. (2013). Insiders' protection of organizational information assets: development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly, `37*(4), 1189-1210.
PwC (2012). Eye of the storm. Key findings from the 2012 global state of information security survey. Retrieved from http://www.cen7dias.es/BOLETINES/330/pwc.pdf
PwC (2014). The global state of information security survey. Retrieved from http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml
Rogers, M., Smoak, N. D., and Liu, J. (2006). Self-reported deviant computer behavior: a big-5, moral choice, and manipulative exploitive behavior analysis. *Deviant Behavior, 27*(3), 245-268.
Rothman, M. and Gandossy, R. (1982). Sad tales: the accounts of white-collar defendants and the decision to sanction. *Pacific Sociological Review, 25*(4), 449-473.
Salleh, N., Hussein, R., Mohamed, N., Karim, N. S. A., Ahlan, A. R., and Aditiawarman, U. (2012). Examining information disclosure behavior on social network sites using protection motivation theory, trust and risk. *Journal of Internet Social Networking & Virtual Communities, 2012*(article ID 281869), 1-11.
Siponen, M. and Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*(3), 487-502.
Smith, A. L., Baxter, R. J., Boss, S. R., and Hunton, J. E. (2012). The dark side of online knowledge sharing. *Journal of Information Systems, 26*(2), 71-91.
Straub, D. W. (1990). Effective IS security. *Information Systems Research, 1*(3), 255-276.
Straub, D. W., Jr. (1986). *Deterring computer abuse: The effectiveness of deterrent countermeasures in the computer security environment.* Unpublished D.B.A., Indiana University, Graduate School of Business, Bloomington, IN.
Straub, D. W. and Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. *MIS Quarterly, 22*(4), 441-469.
Streib, G. and Binstock, R. (1990). Aging and the social sciences: changes in the field. In R. Binstock & L. George (Eds.), *Handbook of Aging and the Social Sciences*. New York, New York: Academic Press.
Sverke, M. and Hellgren, J. (2002). The nature of job insecurity: understanding employment uncertainty on the brink of a new millennium. *Applied Psychology, 51*(1), 23-42.
Thébaud, S. (2010). Masculinity, bargaining, and breadwinning: understanding men's housework in

the cultural context of paid work. *Gender & Society, 24*(3), 330-354.
Vance, A., Lowry, P. B., and Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems, 29*(4), 263-289.
Vance, A., Lowry, P. B., and Eggett, D. (2015). A new approach to the problem of access policy violations: Increasing perceptions of accountability through the user interface. *MIS Quarterly, 39*(2), 345-366.
Wall, J. D., Lowry, P. B., and Barlow, J. (2016). Organizational violations of externally governed privacy and security rules: Explaining and predicting selective violations under conditions of strain and excess. *Journal of the Association for Information Systems, 17*(1), 39-76.
Warkentin, M. E. and Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems, 18*(2), 101-105.
Warren, T. (2007). Conceptualizing breadwinning work. *Work, Employment & Society, 21*(2), 317-336.
Weisburd, D. (1991). *Crimes of the Middle Classes: White Collar Offenders in the Federal Courts*. New Haven, Connecticut: Yale University Press.
Weisburd, D. and Waring, E. (2001). *White-collar Crime and Criminal Careers*. New York, New York: Cambridge University Press.
Weisburd, D., Waring, E., and Chayet, E. (1995). Specific deterrence in a sample of offenders convicted of white-collar crimes. *Criminology, 33*(4), 587-607.
Wheeler, S. (1992). The problem of white-collar crime motivation. In K. Schlegel & D. Weisburd (Eds.), *White Collar Crime Reconsidered* (pp. 108-123). Boston, Massachusetts: Northeastern University Press.
Wheeler, S., Weisburd, D., Waring, E., and Bode, N. (1988). White collar crime and criminals. *American Criminal Law Review, 25*(3), 331-357.
Willison, R. (2006). Understanding the perpetration of employee computer crime in the organisational context. *Information and Organization, 16*(4), 304-324.
Willison, R. and Backhouse, J. (2006). Opportunities for computer crime: considering systems risk from a criminological perspective. *European Journal of Information Systems, 15*(4), 403-414.
Willison, R. and Siponen, M. (2009). Overcoming the insider: reducing employee computer crime through situational crime prevention. *Communications of the ACM, 52*(9), 133-137.
Willison, R. and Warkentin, M. (2013). Beyond deterrence: an expanded view of employee computer abuse. *MIS Quarterly, 37*(1), 1-20.
Willison, R., Warkentin, M., and Johnston, A. C. (2016). Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. *Information Systems Journal, forthcoming*(doi: 10.1111/isj.12129).
Willot, S., Griffin, C., and Torrance, M. (2001). Snakes and ladders: upper-middle class male offenders talk about economic crime. *Criminology, 39*(2), 441-466.
Workman, M. (2007). Gaining access with social engineering: an empirical study of the threat. *Information Systems Security, 16*(6), 315-331.
Workman, M. (2008). Wisecrackers: a theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology, 59*(4), 662-674.
Workman, M., Bommer, W. H., and Straub, D. W. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816.
Zhang, L., Pavur, R., York, P., and Amos, C. (2013). Testing a model of users' Web risk information seeking intention. *Informing Science: The International Journal of an Emerging Transdiscipline, 16*(2013), 1-18.
Zhou, X. and Hou, L. (1999). Children of the cultural revolution: the state and the life course in the People's Republic of China. *American Sociological Review, 64*(1), 12-36.

APPENDIX A. SUMMARY OF THE MAJOR ICA LITERATURE

Citation (Study type)	Criminal/ malicious context?	Participants	DV type	Other theories / constructs	Method	Findings / Application to DT
D'Arcy and Devaraj (2012)	Partial (IS misuse intentions; not strong criminal intent)	Employees, including part-time MBA students	Scenarios (negative)	Informal sanctions as DT extension	Factorial survey	Examined formal sanctions (combined severity/certainty) and added informal sanctions (social desirability and moral beliefs). All three were significant. All participants were given four scenarios and all measures were averaged from the four scenarios and analyzed together.
D'Arcy and Hovav (2007)	Partial (IS misuse intentions; not strong criminal intent)	Employees, including part-time MBA students	Intentions (negative)	n/a	Factorial survey	Did not directly use DT constructs, but argued that ISPs, SETA programs, monitoring, and preventive security software to be deterrence surrogates that reduce IS misuse intentions. All were significant except computer monitoring.
D'Arcy and Hovav (2009)	Partial (unauthorized access/modification intent)	Employees, including part-time MBA students	Intentions (negative)	Moral judgment	Cross-sectional survey	Did not directly use DT constructs, but argued "security countermeasures" of ISPs, acceptable use guidelines, monitoring and SETA programs to be deterrence surrogates that reduce IS misuse intentions. Moral judgement was the strongest factors whereas mixed support was found for the deterrence surrogates
D'Arcy et al. (2009a)	Partial (IS misuse intentions; not strong criminal intent)	Employees	Scenarios (negative)	Moral commitment	Factorial survey	Showed that severity, but not certainty, was associated with decreased IS misuse intentions. Also, added moral commitment as a negative influencer. Other factors were also examined to predict certainty and severity. 4 scenarios: (1) email joke, (2) use restricted info to ask for a raise, (3) unlicensed software, (4) round up work hours. All participants were given four scenarios and all measures were averaged from the four scenarios and analyzed together.
Harrington (1996)	Yes (ICA)	IS employees	Scenarios (negative)	Ethical judgments (denial of responsibility)	Factorial survey	This is not directly a DT study. However, they used corporate codes of ethics as deterrence surrogates in their study and used DT literature to justify this decision. Scenarios involved true criminal computer abuse: cracking, sabotage, purposeful virus spread, software theft, fraud. Showed corporate codes did not reduce intent, however they did serve to reduce denial of responsibility.
Hovav and	Partial (IS misuse	Employees,	Scenarios	Moral beliefs	Factorial	Examined DT in US versus Korea context. All participants

Citation (Study type)	Criminal/ malicious context?	Participants	DV type	Other theories / constructs	Method	Findings / Application to DT
D'Arcy (2012)	intentions; not strong criminal intent)	including part-time MBA students	(negative)		survey	were given four scenarios and all measures were averaged from the four scenarios and analyzed together. Examined severity and certainty. Certainty was significant for US sample but not severity; severity was significant for Korean sample but not certainty.
Hu et al. (2011)	Yes (ICA)	Employees	Scenarios (negative)	RCT, self-control, shame, moral beliefs	Factorial survey	Used certainty, severity, and celerity of sanctions. In model these three directly predicted informal and formal risks. Separate model showing these three against negative intentions showed no significance. Only extrinsic and intrinsic benefits were directly significant. Three computer abuse scenarios: unauthorized access for gain, steal/sell commercial secret, steal/sell product info.
Lee et al. (2004a)	Yes (ICA)	Employees	Intentions & behaviors (negative)	Social control	Cross-sectional survey	Did not use certainty and severity. Instead, used security policy, security awareness, and physical security system all as "general deterrence theory" surrogates. Examined intention from participants and then added reported actual abuse from insiders and outside "invaders." Model deterrence surrogates as predictors of "self-defense intention", which then was significant modelled to decrease abuse by "invaders" and abuse by insiders. Of the surrogates, only "security system" was significant.
Lowry et al. (2014)	Partial (some ICA but not all was criminal)	Employees	Behaviors (negative)	Formalism vs. utilitarianism Collectivism versus individualism	Cross-sectional survey	The purpose of this article was to examine the degree to which ethics (formalisms versus utilitarianism) and culture (collectivism versus individualism) is associated with computer abuse. Those leaning toward formalistic ethics were less likely to commit computer abuse than those leaning toward utilitarianism. Collectivists were less likely to commit computer abuse than individualists.
Lowry et al. (2015)	Partial (some ICA but not all was criminal)	Employees	Behaviors (negative)	Fairness theory	Cross-sectional survey	The primary purpose of the article was testing fairness theory in the context of reactive computer abuse at work. However, the authors tested certainty, severity, and celerity as counter-explanations. They were not significant in this context.
Peace et al. (2003)	Yes (software piracy; form of ICA)	Employees	Attitudes & Intentions	TPB	Cross-sectional	Studied employee software piracy in the workplace. Severity and certainty decreased attitude.

Citation (Study type)	Criminal/ malicious context?	Participants	DV type	Other theories / constructs	Method	Findings / Application to DT
					survey	
Posey et al. (2011)	Partial (some ICA but not all was criminal)	Employees	Behaviors (negative)	Justice theory Reactance theory	Cross-sectional survey	The primary purpose of the article was justice theory and reactance theory in the context of reactive computer abuse at work. Both procedural and distributed justices were associated with increased computer abuse.
Straub (1990)	Yes (ICA)	IS management	Manager report of observed abuse (negative)	Provide basic rival explanations	Cross-sectional survey	Implementing IS security deterrents (measured as certainty and severity) decreased computer abuse. Straub (1986) is the dissertation version of this article and has the same data; thus we summarize them together here.
Straub and Welke (1998)	Yes (ICA)	IS management	Qualitative discussion of risk assessment	n/a	Qual.	Non-empirical qualitative study that used ideas of DT to help cope with and plan for systems risk. Not a direct test of DT, but suggested communicating sanctions as part of SETA programs.
Willison et al. (2016)	Yes (ICA)	Employees	Scenarios (negative)	DT Neutralization theory Justice theory	Factorial survey	Using scenarios, showed employees may form intentions toward computer abuse if they perceive procedural justice, but that this is moderated by neutralization and certainty of sanctions.

[i] To clarify, CERT is not an acronym; it is a name and a registered service mark. "CERT" and "CERT Coordination Center" are registered service marks of Carnegie Mellon University. See http://www.cert.org/

[ii] Willison and Warkentin (2013) stated their Figure 3 p. 5 was adapted from Loch et al. (1992)